

ABSTRACT OF THE INVENTION-

DYNAMIC SOURCE AUTHENTICATION AND ENCRYPTION  
CRYPTOGRAPHIC SCHEME FOR A GROUP-BASED SECURE  
5 COMMUNICATION ENVIRONMENT

Embodiments of the present invention include a method for  
establishing secure group-based communication comprising: distributing a  
first set of keys to a plurality of hosts for encrypting communication and for  
10 source authentication of group-based communication between the plurality of  
hosts. The method further includes distributing a second set of keys to the  
plurality of hosts for dynamically modifying the first set of keys as also any  
other keys used (encryption keys or seed variables) when required (viz. for  
periodic re-keying or for adjusting to a change in group membership).

15